IE4758 Information Security – Assignment 1

Shoon Zhen Yong (U1920283L)

**Introduction**

Since the prevalence of the COVID-19, there is a significance change in the way we live. Daily activities such as working and social meetings have transformed from offline to online platforms. The huge increase in the time we spent on the internet has become a golden opportunity for attackers to exploit the vulnerability of the online users and the online platform(s) they used. Statistics has shown that the number of global internet users has been on the rise ever since the internet was adopted worldwide. 2022’s figure of 4.95 billion marks a 6.2 percent year-over-year, the fastest growth rate since 2019 [1]. This shows the needs of cybersecurity to protect the internet users.

In the context of businesses, companies around the world are adapting to the work-from-home mode. The limitation of face-to-face meetings has resulted in the higher-than-ever dependence on online workspaces and software such as Zoom and Microsoft Teams. While we enjoy the convenience brought by the sophisticated software, the adversaries are targeting every security loophole they found.

**Examples of Ransomware Attack**

Below are some examples of ransomware attack (in chronological order).

1. Cryptolocker

Cryptolocker is a ransomware virus that infects your computer and secretly encrypts office documents, images, and other important files. Once the files are infected, you will receive a message explaining you cannot access your files unless you pay a "fine”.[2] Discovered early in September 2013, Cryptolocker would cripple more than 250,000 computer systems during the following four months. Victims were instructed to send payments in cryptocurrency or money cards to regain access. The ransomware delivered at least $3 million to its perpetrators. [3]

1. SamSam

SamSam ransomware was first detected in late 2015. It made a strong start in 2018, hitting meticulously selected organizations. SamSam was used against particular entities, such as hospitals and educational institutions, which were most likely to pay to get their data back. The criminals behind this ransomware used vulnerabilities to obtain access to the victims’ network or use brute-force tactics against the weak passwords of the Remote Desktop Protocol (RDP). [4]

1. WannaCry

In May 2017, WannaCry ransomware spread globally through computers running Windows. The WannaCry ransomware encrypted Windows computers worldwide and demanded a ransom of initially $300 worth of Bitcoin, later $600. It infected an estimated 230,000 computers across 150 countries in just hours. [5]

**Ransomware Attacks**

Ransomware is a type of malware attack in which the attacker locks and encrypts the victim’s data, important files and then demands a payment to unlock and decrypt the data. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail email. Most ransomware attacks are triggered by tricking users into clicking on deceptive links using social engineering tactics or by exploiting system vulnerabilities. An attacker always demands payment in cryptocurrency as taking payments this way reduces the risk of being caught. Once the payment is secured the victim receives an unlock code or decryption file that releases the data on the computer network, mobile device, or servers.

A typical ransomware attack made up of 7 stages. [6] It is a series of events designed to disrupt and disable systems and to force organizations to pay large sums to recover data and get back online.

**Stage 1 – Initiation of the Attack**

This first stage is where the attacker sets up the ransomware to infiltrate your system. This can be done in several ways, such as sending out phishing email attacks, setting up malicious websites, or attacking software vulnerabilities directly. The more users your organization has, the more vulnerable you are to a user-targeted attack like phishing, malicious websites, or combinations of these. It only takes one user to make a mistake and execute the ransomware code, infiltrating the system.

**Stage 2 – Instantiation**

The second stage occurs once the ransomware has penetrated your system. The malicious code will set up a communication line back to the attacker. The ransomware attacker may download additional malware using this communication line. The ransomware may lie hidden and dormant for a certain period before the attacker initiates the attack. The ransomware may move laterally across other systems in the organization to access as much data as possible. Many ransomware variants now also target backup systems to eliminate the chance for you as the victim to restore data. The victim could be completely unaware that their systems are compromised, and the attacker can wait for the optimal time to launch the attack.

**Stage 3 – Activation**

The third stage is when the attacker remotely activates the ransomware attack. Once the attack has begun, it can be a race against time for the victim to identify that the attack is occurring so that mitigation and recovery efforts may go into action.

**Stage 4 – Encryption**

Ransomware holds data hostage through encryption. Ransomware that targets backup systems may delete or encrypt the backups to prevent recovery. Decrypting the data is highly unlikely so the victim will have three choices: lose the data, recover from a replica or backup, or pay the ransom.

**Stage 5 – Ransom Request**

The victim was presented with information on how to pay a ransom via a cryptocurrency transaction to regain control of their system or data. Depending on what data the ransomware was able to encrypt, data will be inaccessible, and the encryption can disable applications and entire systems. Operations are severely impacted without access to data or services.

**Stage 6 – Recovery or Ransom**

In this stage, many organizations we’ve seen in the news experienced impacts of significant downtime or disruption, and many have chosen to pay a ransom. Without an effective recovery method, even if the data can be recovered, at least partially, the cost of doing so may exceed the cost of paying the ransom. However, suppose your organization has an effective recovery plan in place. In that case, the victim may recover the data quickly with minimal disruption and no need to pay a ransom, eliminating the negative publicity of downtime and paying an exorbitant ransom.

### ****Stage 7 – Clean Up****

Paying a ransom or even recovering data from a backup or replica does not necessarily eliminate the ransomware on the system. The malicious files and code may still be present and need to be removed. The attack itself will likely reveal the type of ransomware and make it easier to locate and purge from the system. If necessary, systems can be recovered in an isolated network to clean up the malware without risking re-activation. Once the malware has been cleaned up, the system can be returned to regular operation.

**Common Types of Ransomware Attacks**

1. **Crypto-ransomware**

The goal of crypto ransomware is to hack and [encrypt](https://us.norton.com/internetsecurity-privacy-what-is-encryption.html) the sensitive files located on the victim’s computer, such as documents, pictures, or videos. While cybercriminals withhold access to these files, they don’t go as far as interfering with basic computer functions like other types of ransomwares. Hackers want to create a sense of panic within the user by allowing them to see their files without the ability to open their information.

1. **Locker ransomware**

Locker ransomware is unique in that it solely aims to lock victims out of their computers. Hackers do this by disabling all basic computer functions with an exception for minor mouse and keyboard capabilities. Leaving the mouse and keyboard somewhat operable lets the user fulfil the demands of the cybercriminal to gain access back into their device.

A common trend with locker ransomware is that it generally doesn’t target specific files. So, the likelihood of data destruction is lower compared to other types of ransomware attacks. However, there are no guarantees when dealing with cybercriminal masterminds.

1. **Scareware**

[Scareware](https://us.norton.com/internetsecurity-online-scams-how-to-spot-online-scareware-scams.html) is a malicious software created to make false claims about viruses infecting a user's computer or device. A payment is typically requested from the owner to solve the falsified issues. While some types of scareware can lock a user out of their device, others will only go as far as flooding the screen with countless pop-ups to overwhelm the user.

1. **Ransomware as a Service (RaaS)**

Ransomware as a Service (RaaS) is a dark web business model created to help ransomware hackers streamline their attacks. Developers created this software to automatically carry out all aspects of a ransomware attack for the cyberthief, from sending out the ransomware to collecting payments and restoring user access

1. **Doxware or Leakware**

[Doxware](https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html), also known as leakware, threatens the distribution of sensitive data online, targeting people and businesses alike. Since hackers know people, and especially businesses, will do almost anything to prevent confidential and [personal data](https://us.norton.com/internetsecurity-privacy-personal-data-leaking-digital-exhaust.html) from falling into the wrong hands, they often demand compensation to prevent its release.

**Protective Measures Against Ransomware Attacks**

1. Government
2. National Cybersecurity Workforce

A study predicated that the cybersecurity workforce would reach a 1.8 million shortage by 2022. [7] Thus, the government needs to focus on training and upskilling the cybersecurity professionals throughout the country. This could achieve by partnering with formal education institutions and establishing training portal to provide free online cybersecurity training

1. Establish National Cybersecurity Agency

The government should establish a national cybersecurity agency that is responsible to define and drive the cybersecurity agenda of the country. For example, The Cyber Security Agency of Singapore (CSA) was formed in 2015 and has been tasked to protect Singapore’s cyberspace [8]. The agency will develop a comprehensive cybersecurity strategy and protect the country’s essential infrastructure, defining the cybersecurity standard and improving the cyber awareness within the country and professional capabilities in cybersecurity.

1. Businesses
2. Setting up cybersecurity policies and provide training to employees

It is crucial for companies to make sure that their employees abide by the cybersecurity policies. Therefore, training should be done to introduce company’s policies, equip them with sufficient cybersecurity knowledge and demonstrate good work ethics that are expected from the employees. The training session is usually set as mandatory for each and every person in the company. One of the practices includes employees would be required to only use their work computer for work purposes or always lock their computer before leaving their desk.

1. Strengthen cybersecurity technologies

The attacker usually exploits unpatched vulnerabilities to gain unauthorized access to systems and networks to launch ransomware attacks. The scanning of the systems and networks should be performed at least once a week to ensure it does not contain malicious files. Additionally, software and application inside the system should update to the latest version and company’s IT must constantly download the latest security patches. Next, the organization should enable strong spam filters and email authentication protocols such as Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) to reduce the risk of phishing emails reaching the user.

1. Individuals

We must always be mindful to everything around us, including the services we use and the people we engage with. We must be careful when clicking any emails from unknown senders. We must always remember to first check for the credibility of the source of the emails before clicking on it. Other than that, we should also not simply giving out our own personal information and password.

Besides, we can install antivirus software to auto-detect malwares in our device. We should not let others to simply take control of our devices, be it physical control or remote access. This is risky as it will give attackers chances to steal our data or inject viruses into our device.

Moreover, we should always keep ourselves updated to the latest cybersecurity news by keeping a lookout at the official information released by the national cybersecurity agency, or read about the previous attacks so that we will be less likely to fall into the trap set by the attackers.

**Conclusion**

Nevertheless, preventing ransomware attacks is a whole process which cannot rely on a single party. We need the effort from the entire society to have the sense of responsibility and consciousness in realizing the importance of each or our role in safeguarding our own’s cybersecurity and privacy.

**References**

[1] Simon Kemp, “Digital 2022: Global Overview Report,” 26-Jan-2022. [Online]. Available: https://datareportal.com/reports/digital-2022-global-overview-report.

[2] “Case study: Cryptolocker ransomware,” Strategy Marketing Agency, 29-Apr-2021. [Online]. Available: https://strategynewmedia.com/cryptolocker-ransomware/.

[3] J. Dossett, “A timeline of the biggest ransomware attacks,” CNET. [Online]. Available: https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-

[4] “5 biggest ransomware attacks in history,” Swiss Cyber Institute, 28-Mar-2022. [Online]. Available: https://swisscyberinstitute.com/blog/5-biggest-ransomware-attacks-in-history/.

[5] “What was Wannacry?: Wannacry ransomware,” Malwarebytes. [Online]. Available: <https://www.malwarebytes.com/wannacry>.

[6] D. Paquette, “The 7 stages of a ransomware attack,” Zerto, 10-May-2022. [Online]. Available: https://www.zerto.com/blog/ransomware-recovery/the-7-stages-of-a-ransomware-attack/.

[7] “CSA: Our organisation,” Cyber Security Agency. [Online]. Available: https://www.csa.gov.sg/Who-We-Are/Our-Organisation.

[8] A. Fadia, M. Nayfeh, and J. Noble, “Follow the leaders: How governments can combat intensifying cybersecurity risks,” McKinsey &amp; Company, 01-Sep-2022. [Online]. Available:https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks.